Status Update: Cook County Information Security

SENSITIVE AND INFORMATION SECURITY RELATED

March 2022

Purpose

The Chief Information Security Officer's (CISO’s) semi – annual report shall detail:

- The status of all Agencies' adoption and compliance with the Information Security Framework (ISF); and
- A summary of all advice and recommendations of each Agency regarding their unique considerations.

Addressed Multiple Cyber Threats – Feb ‘21 to Jul ‘21

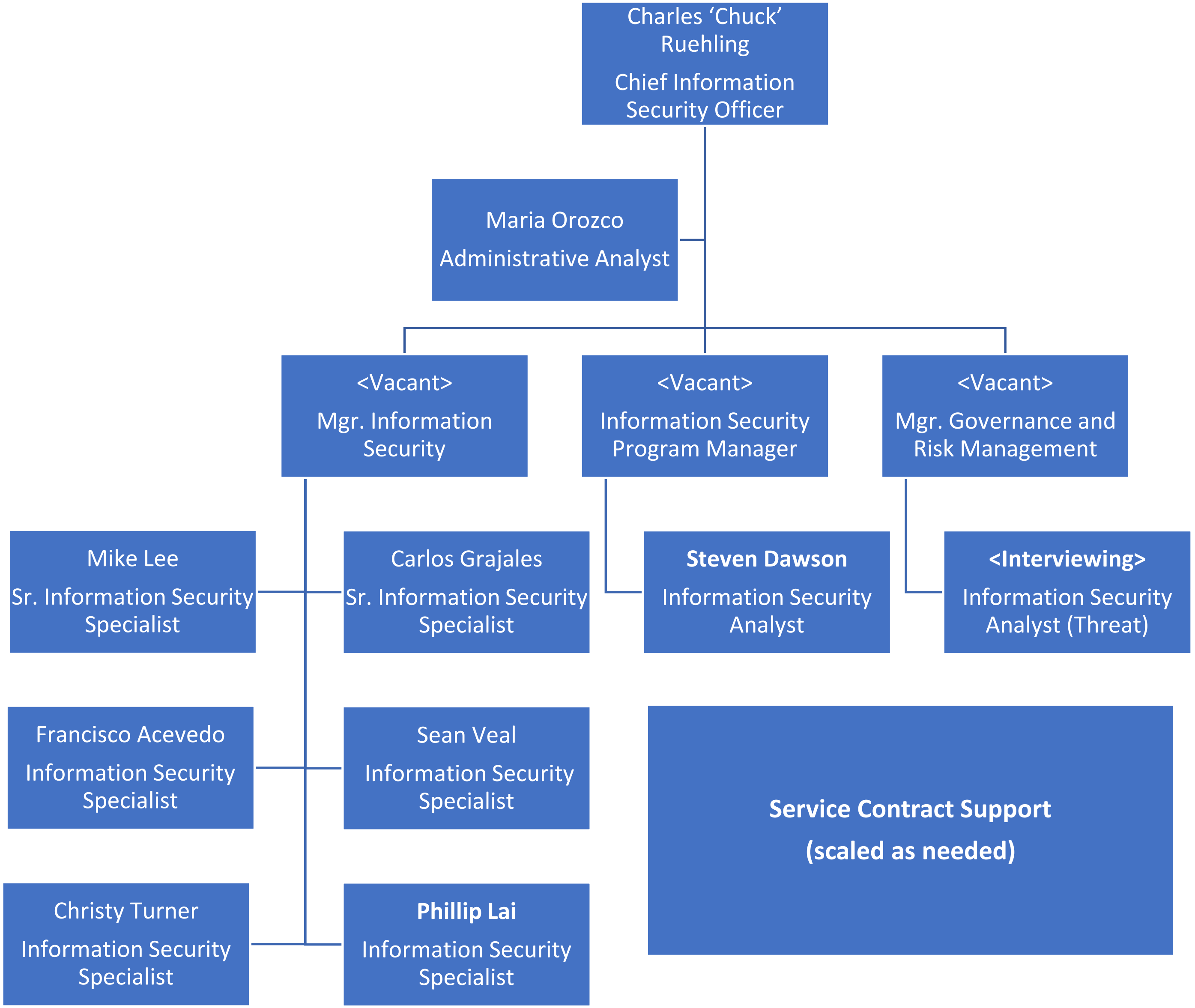
Total Events: 88,322,200,886

Total Security Events: 963,187,038

Incidents (Tickets): 1,226

- EternalBlue Ransomware
- EternalRomance Ransomware
- Eternal Tools
- WannaCry (leveraged EternalBlue and EternalRomance ransomware)
- Bad Rabbit Ransomware
- Petya/NotPetya Ransomware
- Virut Malware
- Kraken Malware
- FakeAV Exploit Kit
- Adobe Acrobat [illegible] Memory Corruption Vulnerability (CVE-2017-3122)
- Adobe Acrobat Professional security bypass vulnerability (CVE-2016-104[illegible]
- Adobe Acrobat Reader Memory Corruption Remote Code Execution (CVE-2017-11238)
- Adobe Acrobat Reader Memory Corruption Vulnerability (CVE-2017-11[illegible]
- Adobe Acrobat Reader Open Type Font File Format Vulnerability
- Adobe Acrobat Reader stack buffer overflow vulnerability (CVE-2017-2948)
- Adobe Acrobat Reader Stack Overflow Vulnerability Denial of Service
- Adobe Acrobat Reader TIFF File [illegible] Overflow Vulnerability (CVE-2017-3049)
- Adobe Acrobat Reader Type Confusion Remote Code Execution (CVE-2017-11221)
- Adobe Acrobat Reader Use After Free Vulnerability (CVE-2016-1089)
- Adobe Acrobat Type Confusion Vulnerability (CVE-2017-16406)
- Adobe Acrobat Use After Free Vulnerability(CVE-2016-0932)
- Cisco Syslog DoS attacks
- Adobe Flash Player – Too many to name individually
- Adobe Reader– Too many to name individually
- Adobe Shockwave Player – Too many to name individually

Information Security Office Organizational Chart



Charles 'Chuck' Ruehling

Chief Information Security Officer

Maria Orozco

Administrative Analyst

<Vacant>

Mgr. Information Security

<Vacant>

Information Security Program Manager

<Vacant>

Mgr. Governance and Risk Management

Mike Lee

Sr. Information Security Specialist

Carlos Grajales

Sr. Information Security Specialist

Steven Dawson

Information Security Analyst

<Interviewing>

Information Security Analyst (Threat)

Francisco Acevedo

Information Security Specialist

Sean Veal

Information Security Specialist

Service Contract Support

(scaled as needed)

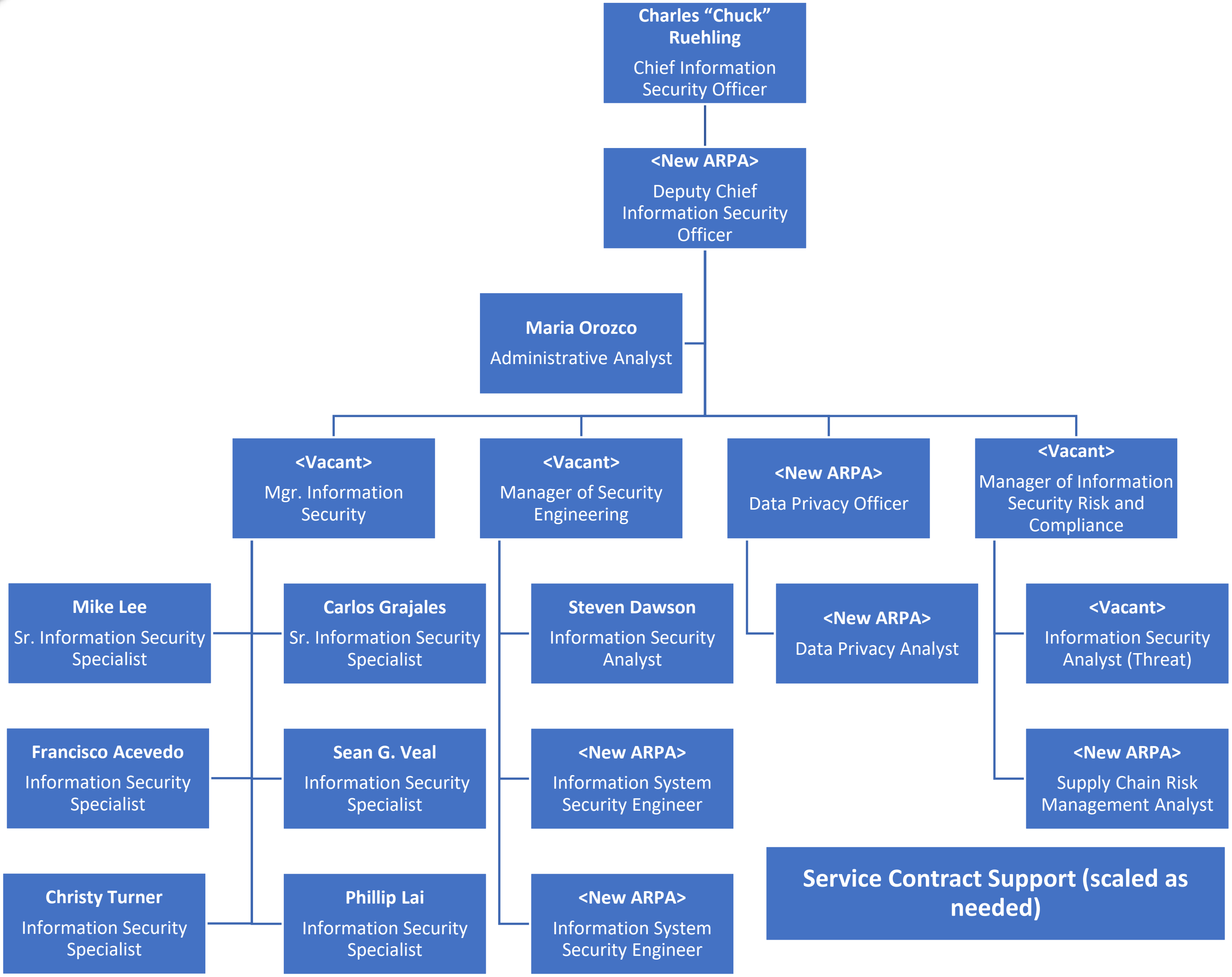
Christy Turner

Information Security Specialist

Phillip Lai

Information Security Specialist

Information Security Office Organizational Chart (ARPA)



Charles "Chuck" Ruehling
Chief Information Security Officer

<New ARPA>
Deputy Chief Information Security Officer

Maria Orozco
Administrative Analyst

<Vacant>
Mgr. Information Security

Mike Lee
Sr. Information Security Specialist

Carlos Grajales
Sr. Information Security Specialist

Francisco Acevedo
Information Security Specialist

Sean G. Veal
Information Security Specialist

Christy Turner
Information Security Specialist

Phillip Lai
Information Security Specialist

<Vacant>
Manager of Security Engineering

Steven Dawson
Information Security Analyst

<New ARPA>
Information System Security Engineer

<New ARPA>
Information System Security Engineer

<New ARPA>
Data Privacy Officer

<New ARPA>
Data Privacy Analyst

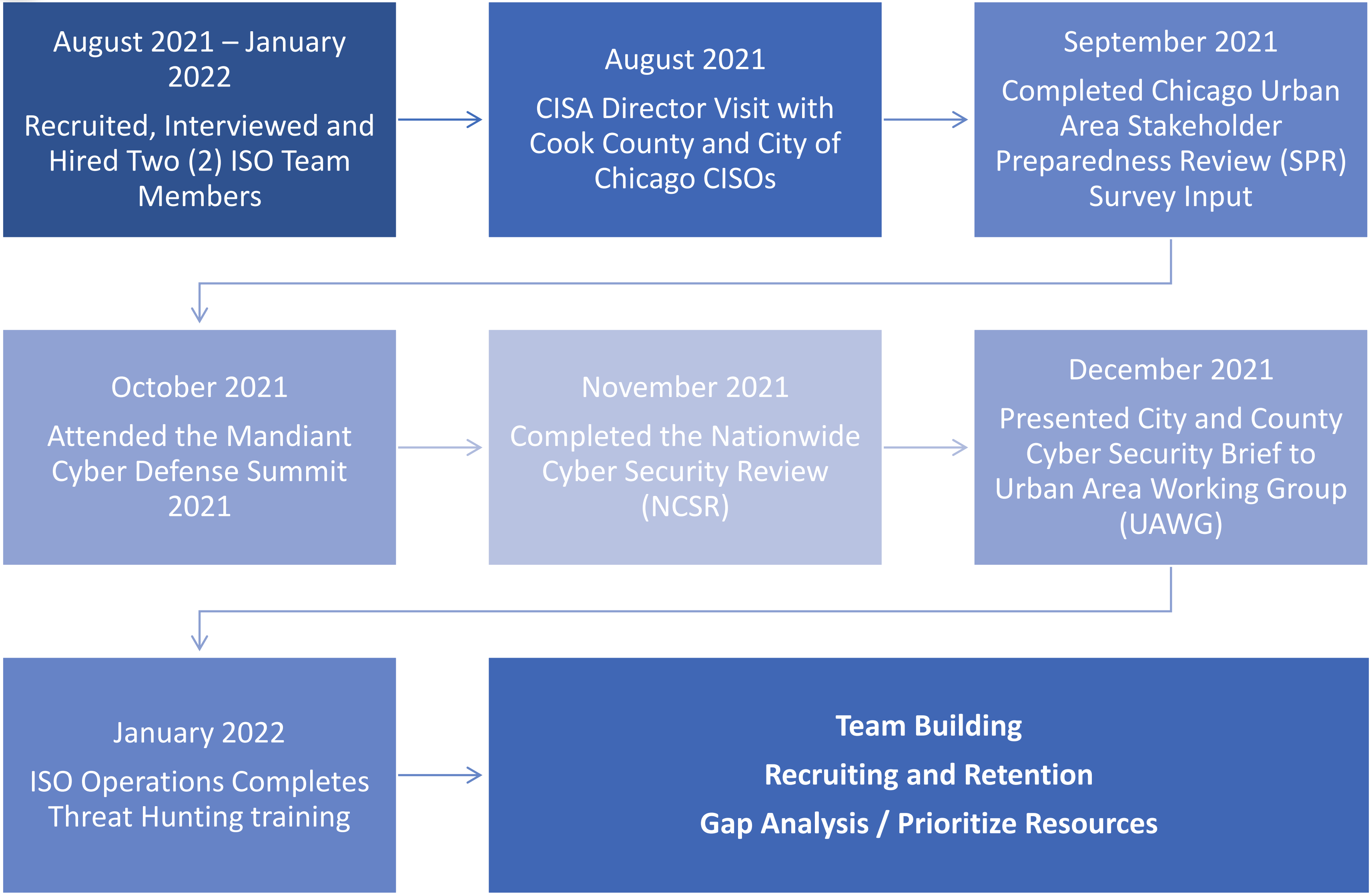
<Vacant>
Manager of Information Security Risk and Compliance

<Vacant>
Information Security Analyst (Threat)

<New ARPA>
Supply Chain Risk Management Analyst

Service Contract Support (scaled as needed)

Information Security Office (ISO) Major Events



August 2021 – January 2022

Recruited, Interviewed and Hired Two (2) ISO Team Members

August 2021

CISA Director Visit with Cook County and City of Chicago CISOs

September 2021

Completed Chicago Urban Area Stakeholder Preparedness Review (SPR) Survey Input

October 2021

Attended the Mandiant Cyber Defense Summit 2021

November 2021

Completed the Nationwide Cyber Security Review (NCSR)

December 2021

Presented City and County Cyber Security Brief to Urban Area Working Group (UAWG)

January 2022

ISO Operations Completes Threat Hunting training

Team Building

Recruiting and Retention

Gap Analysis / Prioritize Resources

Agency Support

Completed Updates of the Information Security Framework Policies Based on the NIST Special Publication (SP) 800-53rev5 – in Total 20 Families

Successfully requested American Rescue Plan Act (ARPA) Funding to mature ISO Organization to incorporate Data Privacy, Security Engineering and Supply Chain Risk Management Capabilities

Began Implementation of Two Factor Authentication (2FA) on Virtual Private Network (VPN) Infrastructure and continued Work with Several Agencies to Integrate Two-Factor Authentication (2FA) into IT Environments

Hosted Vendor Engagements or ISO Security Tool Training with 10 Different Capabilities in ISO Tool Stack

2022 Projects / Events

CYBERSECURITY INCIDENT RESPONSE TABLETOP EXERCISE (TTX)

- Building on the After-Action Report (AAR) and lessons learned from the June 2021 TTX will continue to mature the Cybersecurity Incident Response TTX for 2022

INFRASTRUCTURE REFRESH OF THE SECURITY TOOL STACK

- Capital Budget approved for 2022, the ISO will continue the refresh of the security tool stack that is at end of life for vendor support while evaluating capabilities.

PREPARE FOR INFORMATION SECURITY OFFICE GRANT BUDGET SHORTFALL

- Build the request and justification for some ISO provided security capabilities moving to a fixed charges model as early as Cook County FY 2023.

MATURE E-MAIL SECURITY

- Implement and test new authentication technologies for our e-mail environment DomainKeys Identified Mail, Sender Policy Framework, and Domain-based Message Authentication Reporting and Conformance (DKIM, SPF, and DMARC)

Cyber Security Challenges

Evolving Adversaries & Threats

Cyber Hygiene

Mature Capabilities

Talent Recruitment & Retention

Budget

Information security is a continuous process that requires due diligence, expertise and collaboration from all agencies to ensure that Cook County is adequately prepared for cyber security threats.

A modern cybersecurity program must have Board and Executive level visibility, funding and support.

Questions